

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平 8-237596

(43) 公開日 平成 8 年 (1996) 9 月 13 日

(51) Int. Cl. <sup>6</sup>	識別記号	庁内整理番号	F I	技術表示箇所
H04N 5/91			H04N 5/91	P
5/92			5/92	H
7/167			7/167	

審査請求 未請求 請求項の数 38 OL (全 14 頁)

(21) 出願番号 特願平 7-318398

(22) 出願日 平成 7 年 (1995) 12 月 6 日

(31) 優先権主張番号 1994-33336

(32) 優先日 1994 年 12 月 8 日

(33) 優先権主張国 韓国 (KR)

(71) 出願人 590001669

エルジー電子株式会社

大韓民国, ソウル特別市永登浦区汝矣島洞  
20

(72) 発明者 朴 兌濬

大韓民国, ソウル市, 種路區, 崇仁  
洞, 20-118

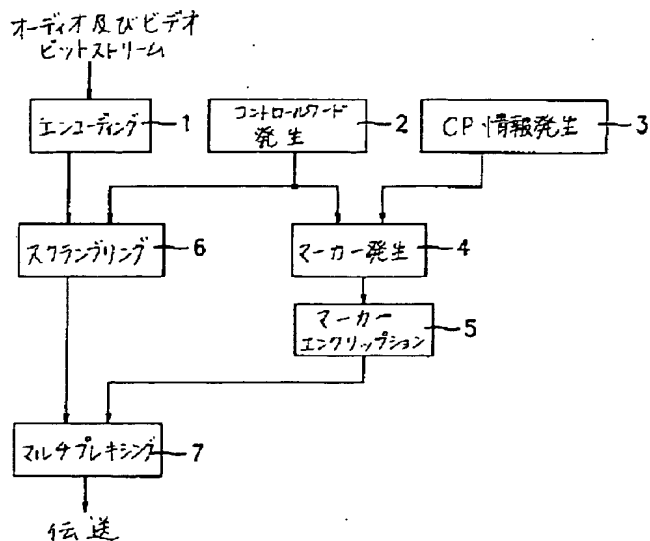
(74) 代理人 弁理士 山本 秀策

(54) 【発明の名称】 デジタル磁気記録再生システムの複写防止方法及び装置

(57) 【要約】

【課題】 プログラム供給者が所望の多様な複写防止機能を実現できるようにしたデジタル磁気記録再生システムの複写防止方法及び装置を提供する。

【解決手段】 本発明によるデジタル磁気記録再生システムの複写防止方法は、オーディオ及びビデオビットストリームをスクランプリングするためのコントロールワードと不法複写防止のための CP 情報により作られたマーカーを暗号化キーを用いてエンクリプションして前記コントロールワードにスクランプリングされたオーディオ及びビデオビットストリームをマルチプレキシングして伝送し、前記伝送されたビットストリームからマーカーを検出し暗号化されたキーを用いてディクリプション及び分析して複写を許容するか否かを決定して検出されたマーカーを更新させビデオテープに記録させ、前記マーカーからコントロールワードを発生してディスクランプリングしてディスプレイできるようにモニターに出力することによりなる。



## 【特許請求の範囲】

【請求項1】 オーディオ及びビデオビットストリームをスクランプリングするためのコントロールワードと不法複写防止のためのコピー防止（CP）情報とにより作られたマーカ―を、暗号化キーを用いてエンクリプションして、前記コントロールワードでスクランプリングされたオーディオ及びビデオビットストリームで、マルチプレキシングして伝送するオーディオ及びビデオ信号伝送工程と、

前記伝送されたビットストリームからマーカ―を検出し、暗号化されたキーを用いてディクリプション及び分析して、複写を許容するか否かを決定して、検出されたマーカ―を更新させビデオテープに記録させ、前記マーカ―からコントロールワードを発生してディスクランプリングして、ディスプレイできるようにモニターに出力するオーディオ及びビデオ信号受信及び記録工程と、を包含するデジタル磁気記録再生システムの複写防止方法。

【請求項2】 前記マーカ―は、前記ビットストリーム内の伝送プライベートデータフィールドに位置する請求項1に記載のデジタル磁気記録再生システムの複写防止方法。

【請求項3】 前記マーカ―は、不法複写防止のためのコピー防止（CP）情報の記録されたコピー防止（CP）情報領域と、ディスクランプリングのためのコントロールワードが記録されたコントロールワード領域と、を有する請求項2に記載のデジタル磁気記録再生システムの複写防止方法。

【請求項4】 前記マーカ―は、8バイトよりなる請求項3に記載のデジタル磁気記録再生システムの複写防止方法。

【請求項5】 前記コピー防止（CP）情報領域は、1バイトよりなる請求項4に記載のデジタル磁気記録再生システムの複写防止方法。

【請求項6】 前記コントロールワード領域は、4バイトよりなる請求項4に記載のデジタル磁気記録再生システムの複写防止方法。

【請求項7】 前記コピー防止（CP）情報は、プログラムの複写可能回数を制限する世代複写制御フィールドを含めてフォーマッティングされる請求項3に記載のデジタル磁気記録再生システムの複写防止方法。

【請求項8】 前記世代複写制御フィールドは、プログラムの複写を許す回数を制限するための許容世代フィールドと、複写されたプログラムの現在の世代を示す現在世代フィールドと、を有する請求項7に記載のデジタル磁気記録再生システムの複写防止方法。

【請求項9】 前記オーディオ及びビデオ伝送工程は、オーディオ及びビデオビットストリームをエンコーデ

ングするオーディオ及びビデオビットストリームエンコーディング工程と、

スクランプリングのためのコントロールワードを発生するコントロールワード発生工程と、

前記発生されたコントロールワードを用いて前記エンコーディングされたオーディオ及びビデオビットストリームをスクランプリングするスクランプリング工程と、

不法複写防止のためのコピー防止（CP）情報を発生するコピー防止（CP）情報発生工程と、

10 前記発生されたコントロールワードと前記コピー防止（CP）情報を用いてマーカ―を発生し暗号化されたキーを用いてエンクリプションするマーカ―発生及びエンクリプション工程と、

前記スクランプリングされたオーディオ及びビデオビットストリームとエンクリプションされたマーカ―をマルチプレキシングして伝送するマルチプレキシング及び伝送工程と、

を包含する請求項1に記載のデジタル磁気記録再生システムの複写防止方法。

20 【請求項10】 前記オーディオ及びビデオ信号受信工程は、

前記伝送されたビットストリームをディマルチプレキシングしてマーカ―を検出し、暗号化されたキーを用いてディクリプションするマーカ―検出工程と、

前記検出されたマーカ―を分析して複写を許容するか否かを決定しコントロールワードを検出するマーカ―分析工程と、

前記検出されたコントロールワードで、前記伝送されたオーディオ及びビデオビットストリームをディスクランプリング及びディコーディングして、音声及び映像信号を出力するオーディオ及びビデオディコーディング工程と、

30 前記マーカ―分析結果複写可能な場合、前記検出されたマーカ―を、更新させ暗号化されたキーを用いてエンクリプションして挿入するマーカ―挿入工程と、

を包含する請求項1に記載のデジタル磁気記録再生システムの複写防止方法。

【請求項11】 前記マーカ―分析工程は、前記検出されたマーカ―から不法複写防止のためのコピー防止（CP）情報を検出するコピー防止（CP）情報検出工程と、

前記検出されたコピー防止（CP）情報内のプログラムの複写を許容する回数を制限するための許容世代フィールドの許容世代と、複写されたプログラムの現在の世代を示す現在世代フィールドの現在世代とを比較して、複写が可能か否かを判別して処理する複写回数制限工程と、前記検出されたマーカ―より、ディスクランプリングのためのコントロールワードを検出するコントロールワード検出工程と、

50 を包含する請求項10に記載のデジタル磁気記録再生

システムの複写防止方法。

【請求項 1 2】 前記複写回数制限工程は、前記許容世代フィールドの許容世代と、現在世代フィールドの現在世代とを比較して、前記許容世代が現在世代以下かを判断する工程と、前記判断結果前記許容世代が現在世代以下なら複写を不可能にする工程と、前記判断結果前記許容世代が現在世代以下でなければ複写を可能にし、前記マーカ挿入工程に進む工程と、を包含する請求項 1 1 に記載のデジタル磁気記録再生システムの複写防止方法。

【請求項 1 3】 前記複写を不可能にする工程は、複写後、再生が不可能になるようにコントロールワードを破壊したり、出力できないようにする請求項 1 2 に記載のデジタル磁気記録再生システムの複写防止方法。

【請求項 1 4】 前記コントロールワードは、周期的に変化される請求項 1 0 に記載のデジタル磁気記録再生システムの複写防止方法。

【請求項 1 5】 前記コントロールワードは、0. 6 秒間隔に変わる請求項 1 4 に記載のデジタル磁気記録再生システムの複写防止方法。

【請求項 1 6】 前記マーカは、前記コントロールワードが変わる毎に、前記ビットストリーム内のプライベートデータフィールドに位置する請求項 1 4 に記載のデジタル磁気記録再生システムの複写防止方法。

【請求項 1 7】 前記マーカ挿入工程は、前記マーカ分析結果複写可能な場合は前記マーカを更新させる工程と、前記更新されたマーカを暗号化されたキーを用いてエンクリプションする工程と、前記エンクリプションされたマーカを次に現れるマーカと交替して挿入する工程と、を包含する請求項 1 6 に記載のデジタル磁気記録再生システムの複写防止方法。

【請求項 1 8】 前記暗号化されたキーは、別途の伝送路を通じて伝送され貯蔵される請求項 1 に記載のデジタル磁気記録再生システムの複写防止方法。

【請求項 1 9】 前記暗号化されたキーは、一定間隔に別途の伝送路を通じて伝送され貯蔵される請求項 1 8 に記載のデジタル磁気記録再生システムの複写防止方法。

【請求項 2 0】 入力されるビットストリームから、マーカを検出し、更新されたマーカを、前記ビットストリームに挿入して出力するマーカ検出及び挿入部と、前記マーカ検出及び挿入部から出力されるエンクリプションされたマーカを、暗号化されたキーを用いてディクリプションし分析して、ビットストリームをディスクランプリングさせるためのコントロールワードを出力して、ディクリプションされたマーカを、更新

させ暗号化されたキーを用いてエンクリプションさせ出力するマーカ分析及び処理部と、

前記マーカ分析及び処理部から出力されるコントロールワードと、更新されエンクリプションされたマーカとをバッファリングして、前記更新されエンクリプションされたマーカを、前記マーカ検出及び挿入部で挿入できるように出力するバッファと、

前記バッファから出力されるコントロールワードを用いて、前記マーカ検出及び挿入部を通じて出力されるビットストリームを、ディスクランプリングするディスクランブラと、

を備えたデジタル磁気記録再生システムの複写防止装置。

【請求項 2 1】 前記暗号化されたキーは、別途の伝送路を通じて伝送され貯蔵される請求項 2 0 に記載のデジタル磁気記録再生システムの複写防止装置。

【請求項 2 2】 前記暗号化されたキーは、一定間隔に別途の伝送路を通じて伝送され貯蔵される請求項 2 1 に記載のデジタル磁気記録再生システムの複写防止装置。

【請求項 2 3】 前記マーカは、前記ビットストリーム内の伝送プライベートデータフィールドに位置する請求項 2 0 に記載のデジタル磁気記録再生システムの複写防止装置。

【請求項 2 4】 前記マーカは、不法複写防止のためのコピー防止 (C P) 情報が記録されたコピー防止 (C P) 情報領域と、ディスクランプリングのためのコントロールワードの記録されたコントロールワード領域と、を備えた請求項 2 3 に記載のデジタル磁気記録再生システムの複写防止装置。

【請求項 2 5】 前記マーカは、8 バイトよりなる請求項 2 4 に記載のデジタル磁気記録再生システムの複写防止装置。

【請求項 2 6】 前記コピー防止 (C P) 情報領域は、1 バイトよりなる請求項 2 5 に記載のデジタル磁気記録再生システムの複写防止装置。

【請求項 2 7】 前記コントロールワード領域は、4 バイトよりなる請求項 2 5 に記載のデジタル磁気記録再生システムの複写防止装置。

【請求項 2 8】 前記コピー防止 (C P) 情報は、プログラムの複写可能回数を制限する世代複写制御フィールドを含めてフォーマットされる請求項 2 4 に記載のデジタル磁気記録再生システムの複写防止装置。

【請求項 2 9】 前記世代複写制御フィールドは、プログラムの複写を許容する回数を制限するための許容世代フィールドと、複写されたプログラムの現在の世代を示す現在世代フィールドと、を備えた請求項 2 8 に記載のデジタル磁気記録再生システムの複写防止装置。

【請求項 3 0】 前記コントロールワードは、周期的に変わる請求項 2 0 に記載のデジタル磁気記録再生シス

テムの複写防止装置。

【請求項 3 1】 前記コントロールワードは、0. 6 秒間隔に変わる請求項 3 0 に記載のデジタル磁気記録再生システムの複写防止装置。

【請求項 3 2】 前記マーカは、前記コントロールワードが変わる毎に前記ビットストリーム内のプライベートデータフィールドに位置する請求項 3 0 に記載のデジタル磁気記録再生システムの複写防止装置。

【請求項 3 3】 前記マーカ検出及び挿入部は、前記更新されたマーカを次に現れるマーカと交替して挿入する請求項 3 2 に記載のデジタル磁気記録再生システムの複写防止装置。

【請求項 3 4】 前記マーカ検出及び挿入部は、入力されるビットストリームからエンクリプトされたマーカを検出して、前記マーカ分析及び処理部に出力し、前記ビットストリーム内におけるエンクリプトされたマーカの位置を知らせるマーカ検出フラグ信号を前記ディスクランブラに出力して、前記ディスクランブラが初期化される基準信号として使われるようにし、ビットストリームを出力するマーカ検出部と、前記マーカ検出部から出力されるマーカ検出フラグ信号に応じて、前記マーカ検出部から出力されるビットストリームに、前記バッファから出力される更新されエンクリプションされたマーカを、挿入して、前記ディスクランブラに出力するマーカ挿入部と、を備えた請求項 2 0 に記載のデジタル磁気記録再生システムの複写防止装置。

【請求項 3 5】 前記マーカ分析及び処理部は、前記マーカ検出及び挿入部から出力されるエンクリプションされたマーカを、暗号化されたキーを用いてディクリプションするマーカ解読部と、前記マーカ解読部から出力されるマーカ内部のコピー防止 (CP) 情報を分析して、複写が許容される場合、前記バッファにコントロールワードを出力しマーカを更新するための制御信号を出力するマーカ分析部と、前記マーカ分析部から出力される制御信号に応じて、前記マーカ解読部から出力されるマーカを、更新させ、前記暗号化キーを用いてエンクリプションして、前記バッファに出力するマーカ更新及び暗号化部と、を備えた請求項 2 4 に記載のデジタル磁気記録再生システムの複写防止装置。

【請求項 3 6】 前記マーカ分析及び処理部は、暗号化キーを貯蔵して前記マーカ解読部とマーカ更新及び暗号化部に出力する暗号化キー貯蔵部をさらに備えた請求項 3 5 に記載のデジタル磁気記録再生システムの複写防止装置。

【請求項 3 7】 前記マーカ分析部は、前記コピー防止 (CP) 情報内のプログラムの複写を許容する回数を制限するための許容世代フィールドの許容世代と、複写

されたプログラムの現在の世代を示す現在世代フィールドの現在世代とを比較して、複写が可能か否かを判別する請求項 3 5 に記載のデジタル磁気記録再生システムの複写防止装置。

【請求項 3 8】 前記バッファは、前記マーカ分析及び処理部から出力される更新されエンクリプションされたマーカを一時貯蔵した後前記マーカ検出及び挿入部に出力するマーカバッファと、

10 前記マーカ分析及び処理部から出力されるコントロールワードを一時貯蔵した後前記ディスクランブラに出力するコントロールワードバッファと、を備えた請求項 2 0 に記載のデジタル磁気記録再生システムの複写防止装置。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】 本発明は、デジタル記録再生システムの複写防止方法及び装置に関する。特に、複写防止機能に対する情報と機能実行のためのマーカ (Marker) を暗号化し挿入して、複写防止機能を行い、プログラム供給者の所望の多様な複写防止機能が実現できるデジタル磁気記録再生システムの複写防止方法及び装置に関する。

【0 0 0 2】

【従来の技術】 従来の複写防止方法は、米国特許第 4、8 1 9、0 9 8 号に挙げられている。この方法は、VCR 内の自動利得制御 (AGC) 回路に干渉を起こす信号をビデオ波形に挿入して、テープに記録する方法である。この方法において、上記テープを再生して TV を通じて視聴する場合、干渉信号は、TV の AGC 回路に影響を与えず、正常のディスプレイが可能である。

【0 0 0 3】 しかし、再生された信号を他の VCR が録画する場合、すなわち複写する場合、干渉信号が録画する VCR の AGC 回路に干渉を起こすことにより、不正確な信号レベルを記録させる。したがって、複写されたテープを再生する場合、正常のディスプレイはできない。他の例として、米国特許第 4、5 7 1、6 4 2 号は、再生中 VCR 内のサーボ回路を同期させるに使われるコントロールトラックを用いて、複写防止機能を実現した特許である。この特許の原理は、他のテープで複写する時、コントロールトラックが不正確に記録されるように、ビデオ信号を変化させることである。

【0 0 0 4】 さらに、他の例として、米国特許第 4、5 7 7、2 1 6 号は、ビデオ信号のクロマバースト部分に、位相ノイズのようなものを挿入して複写防止機能を実現している。

【0 0 0 5】

【発明が解決しようとする課題】 上記のような方法は、すべて TV 回路とこれに対応する VCR の回路との間の感度の差を用いる方法である。従って、このような方法

で複写防止されたテープは、一部のVCRでは複写防止できない場合があり、一部のTVでは原本も正常的にディスプレイできない短所がある。

【0006】また、上記のような方法は、アナログ方式の複写防止方法である。このようなアナログ方式の複写防止方法は、NTSC級映像についてアナログVCRへの複写を防ぐにおいて有用な方法である。しかし、ATVの高解像度映像の場合は、アナログVCRよりはデジタルVCRを用いた複写がされるので、アナログ方式の複写防止方法を適用し難い問題点がある。

【0007】従って、本発明の目的は、デジタルTVに適用できる多様な複写防止機能と共に、プログラム供給者が望む複写防止機能を選択できるようにしたデジタル磁気記録再生システムの複写防止方法及び装置を提供することにある。

【0008】

【課題を解決するための手段】本発明によるデジタル磁気記録再生システムの複写防止方法は、オーディオ及びビデオビットストリームをスクランプリングするためのコントロールワードと不法複写防止のためのコピー防止(CP)情報とにより作られたマーカーを、暗号化キーを用いてエンクリプションして、前記コントロールワードでスクランプリングされたオーディオ及びビデオビットストリームで、マルチプレキシングして伝送するオーディオ及びビデオ信号伝送工程と、前記伝送されたビットストリームからマーカーを検出し、暗号化されたキーを用いてディクリプション及び分析して、複写を許容するか否かを決定して、検出されたマーカーを更新させビデオテープに記録させ、前記マーカーからコントロールワードを発生してディスクランプリングして、ディスプレイできるようにモニターに出力するオーディオ及びビデオ信号受信及び記録工程と、を備えており、そのことにより上記目的が達成される。

【0009】ある実施形態では、前記マーカーは、前記ビットストリーム内の伝送プライベートデータフィールドに位置する。

【0010】ある実施形態では、前記マーカーは、不法複写防止のためのコピー防止(CP)情報の記録されたコピー防止(CP)情報領域と、ディスクランプリングのためのコントロールワードが記録されたコントロールワード領域と、を有している。

【0011】ある実施形態では、前記マーカーは、8バイトよりなる。

【0012】ある実施形態では、前記コピー防止(CP)情報領域は、1バイトよりなる。ある実施形態では、前記コントロールワード領域は、4バイトよりなる。

【0013】ある実施形態では、前記コピー防止(CP)情報は、プログラムの複写可能回数を制限する世代複写制御フィールドを含めてフォーマットされ

る。

【0014】ある実施形態では、前記世代複写制御フィールドは、プログラムの複写を許す回数を制限するための許容世代フィールドと、複写されたプログラムの現在の世代を示す現在世代フィールドと、を有している。

【0015】ある実施形態では、前記オーディオ及びビデオ伝送工程は、オーディオ及びビデオビットストリームをエンコーディングするオーディオ及びビデオビットストリームエンコーディング工程(1)と、スクランプリングのためのコントロールワードを発生するコントロールワード発生工程(2)と、前記発生されたコントロールワードを用いて前記エンコーディングされたオーディオ及びビデオビットストリームをスクランプリングするスクランプリング工程(6)と、不法複写防止のためのコピー防止(CP)情報を発生するコピー防止(CP)情報発生工程(3)と、前記発生されたコントロールワードと前記コピー防止(CP)情報を用いてマーカーを発生し暗号化されたキーを用いてエンクリプションするマーカー発生及びエンクリプション工程(4、5)と、前記スクランプリングされたオーディオ及びビデオビットストリームとエンクリプションされたマーカーをマルチプレキシングして伝送するマルチプレキシング及び伝送工程と、を包含している。

【0016】ある実施形態では、前記オーディオ及びビデオ信号受信工程は、前記伝送されたビットストリームをディマルチプレキシングしてマーカーを検出し、暗号化されたキーを用いてディクリプションするマーカー検出工程(11、12)と、前記検出されたマーカーを分析して複写を許容するか否かを決定しコントロールワードを検出するマーカー分析工程(13)と、前記検出されたコントロールワードで、前記伝送されたオーディオ及びビデオビットストリームをディスクランプリング及びディコーディングして、音声及び映像信号を出力するオーディオ及びビデオディコーディング工程(14、15)と、前記マーカー分析結果複写可能な場合、前記検出されたマーカーを、更新させ暗号化されたキーを用いてエンクリプションして挿入するマーカー挿入工程(16、17、18)と、を包含している。

【0017】ある実施形態では、前記マーカー分析工程(13)は、前記検出されたマーカーから不法複写防止のためのコピー防止(CP)情報を検出するコピー防止(CP)情報検出工程と、前記検出されたコピー防止

(CP)情報内のプログラムの複写を許容する回数を制限するための容世代フィールドの許容世代と、複写されたプログラムの現在の世代を示す現在世代フィールドの現在世代とを比較して、複写が可能か否かを判別して処理する複写回数制限工程と、前記検出されたマーカーより、ディスクランプリングのためのコントロールワードを検出するコントロールワード検出工程と、を包含している。

10

20

30

40

50

【0018】ある実施形態では、前記複写回数制限工程は、前記許容世代フィールドの許容世代と、現在世代フィールドの現在世代とを比較して、前記許容世代が現在世代以下かを判断する工程と、前記判断結果前記許容世代が現在世代以下なら複写を不可能にする工程と、前記判断結果前記許容世代が現在世代以下でなければ複写を可能にし、前記マーカー挿入工程に進む工程と、を包含している。

【0019】ある実施形態では、前記複写を不可能にする工程は、複写後、再生が不可能になるようにコントロールワードを破壊したり、出力できないようにする。

【0020】ある実施形態では、前記コントロールワードは、周期的に変化される。

【0021】ある実施形態では、前記コントロールワードは、0.6秒間隔に変わる。

【0022】ある実施形態では、前記マーカーは、前記コントロールワードが変わる毎に、前記ビットストリーム内のプライベートデータフィールドに位置する。

【0023】ある実施形態では、前記マーカー挿入工程は、前記マーカー分析結果複写可能な場合は前記マーカーを更新させる工程（16）と、前記更新されたマーカーを暗号化されたキーを用いてエンクリプションする工程（17）と、前記エンクリプションされたマーカーを次に現れるマーカーと交替して挿入する工程（18）と、を包含している。

【0024】ある実施形態では、前記暗号化されたキーは、別途の伝送路を通じて伝送され貯蔵される。

【0025】ある実施形態では、前記暗号化されたキーは、一定間隔に別途の伝送路を通じて伝送され貯蔵される。

【0026】本発明によるデジタル磁気記録再生システムの複写防止装置は、入力されるビットストリームから、マーカーを検出し、更新されたマーカーを、前記ビットストリームに挿入して出力するマーカー検出及び挿入部と、前記マーカー検出及び挿入部から出力されるエンクリプションされたマーカーを、暗号化されたキーを用いてディクリプションし分析して、ビットストリームをディスクランプリングさせるためのコントロールワードを出力し、ディクリプションされたマーカーを、更新させ暗号化されたキーを用いてエンクリプションさせ出力するマーカー分析及び処理部と、前記マーカー分析及び処理部から出力されるコントロールワードと、更新されエンクリプションされたマーカーとをバッファリングして、前記更新されエンクリプションされたマーカーを、前記マーカー検出及び挿入部で挿入できるように出力するバッファと、前記バッファから出力されるコントロールワードを用いて、前記マーカー検出及び挿入部を通じて出力されるビットストリームを、ディスクランプリングするディスクランブラと、備えており、そのことにより上記目的が達成される。ある実施形

態では、前記暗号化されたキーは、別途の伝送路を通じて伝送され貯蔵される。

【0027】ある実施形態では、前記暗号化されたキーは、一定間隔に別途の伝送路を通じて伝送され貯蔵される。

【0028】ある実施形態では、前記マーカーは、前記ビットストリーム内の伝送プライベートデータフィールドに位置する。

【0029】ある実施形態では、前記マーカーは、不法複写防止のためのコピー防止（CP）情報が記録されたコピー防止（CP）情報領域と、ディスクランプリングのためのコントロールワードの記録されたコントロールワード領域と、を備えている。

【0030】ある実施形態では、前記マーカーは、8バイトよりなる。

【0031】ある実施形態では、前記コピー防止（CP）情報領域は、1バイトよりなる。ある実施形態では、前記コントロールワード領域は、4バイトよりなる。

【0032】ある実施形態では、前記コピー防止（CP）情報は、プログラムの複写可能回数を制限する世代複写制御フィールドを含めてフォーマットされる。

【0033】ある実施形態では、前記世代複写制御フィールドは、プログラムの複写を許容する回数を制限するための許容世代フィールドと、複写されたプログラムの現在の世代を示す現在世代フィールドと、を備えている。

【0034】ある実施形態では、前記コントロールワードは、周期的に変わる。

【0035】ある実施形態では、前記コントロールワードは、0.6秒間隔に変わる。

【0036】ある実施形態では、前記マーカーは、前記コントロールワードが変わる毎に前記ビットストリーム内のプライベートデータフィールドに位置する。

【0037】ある実施形態では、前記マーカー検出及び挿入部は、前記更新されたマーカーを次に現れるマーカーと交替して挿入する。

【0038】ある実施形態では、前記マーカー検出及び挿入部は、入力されるビットストリームからエンクリプトされたマーカーを検出して、前記マーカー分析及び処理部に出力し、前記ビットストリーム内におけるエンクリプトされたマーカーの位置を知らせるマーカー検出フラグ信号を、前記ディスクランブラに出力して、前記ディスクランブラが初期化される基準信号として使われるようにしビットストリームを出力するマーカー検出部と、前記マーカー検出部から出力されるマーカー検出フラグ信号に応じて、前記マーカー検出部から出力されるビットストリームに、前記バッファから出力される更新されエンクリプションされたマーカーを挿入して、前

記ディスクランブラに出力するマーカー挿入部と、を備えている。ある実施形態では、前記マーカー分析及び処理部は、前記マーカー検出及び挿入部から出力されるエンクリプションされたマーカーを、暗号化されたキーを用いてディクリプションするマーカー解読部と、前記マーカー解読部から出力されるマーカー内部のコピー防止 (CP) 情報を分析して、複写が許容される場合、前記バッファにコントロールワードを出力しマーカーを更新するための制御信号を出力するマーカー分析部と、前記マーカー分析部から出力される制御信号に応じて、前記マーカー解読部から出力されるマーカーを、更新させ、前記暗号化キーを用いてエンクリプションして、前記バッファに出力するマーカー更新及び暗号化部と、を備えている。

【0039】ある実施形態では、前記マーカー分析及び処理部は、暗号化キーを貯蔵して前記マーカー解読部とマーカー更新及び暗号化部に出力する暗号化キー貯蔵部をさらに備えている。

【0040】ある実施形態では、前記マーカー分析部は、前記コピー防止 (CP) 情報内のプログラムの複写を許容する回数を制限するための許容世代フィールドの許容世代と、複写されたプログラムの現在の世代を示す現在世代フィールドの現在世代とを比較して、複写が可能か否かを判別する。

【0041】ある実施形態では、前記バッファは、前記マーカー分析及び処理部から出力される更新されエンクリプションされたマーカーを一時貯蔵した後前記マーカー検出及び挿入部に出力するマーカーバッファと、前記マーカー分析及び処理部から出力されるコントロールワードを一時貯蔵した後前記ディスクランブラに出力するコントロールワードバッファと、を備えている。

【0042】

【発明の実施の形態】本発明によるデジタル磁気記録再生システムの複写防止方法及び装置は、DVCRが色々の信号を全部ビデオテープに録画できることを強調して、入力される多種の信号を大きく二種に分類し、各信号別に異なる複写防止機能を実行させる。本発明による上記方法は、まず、地上(Terrestrial)放送、衛星放送、ケーブルから伝送される信号を放送信号に分類し、この信号を録画する時は次のように三種の複写防止機能を有する。この三種の複写防止機能は、テープへの録画絶対不可機能、テープへの自由な録画及び複写許容機能、及びビデオテープへの1世代録画可能と録画されたテープの複写不可機能に分かれる。

【0043】ここで、三番目の機能であるビデオテープへの1世代録画可能と録画されたテープの複写不可機能は、TV受信機から送られる信号をテープで1回録画するのは可能である。1回録画されたテープを再生する場合視聴できるが、他のDVCRでこの信号を録画することは不可能である。

【0044】二番目の分類は、レンタルテープであって、記録媒体に記録された信号に分類する。この信号を録画する時の複写防止機能は、前述したテープへの録画絶対不可機能及びテープへの自由な録画及び複写許容機能と類似であり、次のような三種の複写防止機能を有する。この三種の複写防止機能は、他のテープへの複写絶対不可、他のテープへの自由な複写許容、及び他のテープへの1世代複写許容に分かれる。ここで、他のテープへの1世代複写許容機能は、レンタルテープ原本からは複写本が作られるが、複写本からさらに他の複写本を作ること防ぐ方法であり、DATで使われる複写防止機能である。

【0045】本発明は、上記の機能をプログラム供給者がプログラム供給時に選択できるようにする長所を有する。このため、プログラム供給者は、所望の複写防止機能に対する情報、すなわちマーカーをプログラム内の定められたフィールドに挿入してプログラムを分配する。プログラム供給者が伝送データ上に挿入して伝送するマーカーは、暗号化されている。マーカーを解読できる暗号キーは、不法複写を防ぐために、一定間隔に、例えば一か月に1回ほど、電話線のような別途の伝送路を通じて伝送され、複写防止装置内に貯蔵される。

【0046】上記の複写防止機能を実現する複写防止装置は、ATVディコーダとデジタルVCRが一体型のシステムにおいて、ATVディコーダとデジタルVCRとの間のインタフェース過程で、デジタル複写防止機能を行わせ、受信された暗号化キーを用いて、受信されたプログラムのマーカーを解読し判断して、それぞれの複写防止機能による他の機能を行う。

【0047】本発明によるデジタル磁気記録再生システムの複写防止方法は、図1に示したオーディオ及びビデオ信号伝送工程と、図2に示したオーディオ及びビデオ信号受信及び記録工程により行われる。

【0048】オーディオ及びビデオ信号伝送工程は、オーディオ及びビデオビットストリームをスクランプリングするためのコントロールワードと、不法複写防止のためのコピー防止 (CP) (Copy Protection) 情報により、作られたマーカーを、暗号化されたキーを用いてエンクリプションして、コントロールワードにスクランプリングされたオーディオ及びビデオビットストリームで、マルチプレキシングして伝送することである。プログラム製作者によって、マーカーが作られた状態であり、オーディオ及びビデオビットストリームと共に、マルチプレキシングされ伝送される。

【0049】すなわち、オーディオ及びビデオ信号伝送工程は、図1に示したように、オーディオ及びビデオビットストリームをエンコーディングするオーディオ及びビデオビットストリームエンコーディング工程 (1)、スクランプリングのためのコントロールワードを発生するコントロールワード発生工程 (2)、発生されたコン

トロールワードを用いて、前記エンコーディングされたオーディオ及びビデオビットストリームをスクランプリングするスクランプリング工程(6)、不法複写防止のためのコピー防止(CP)情報を発生するコピー防止

(CP)情報発生工程(3)、発生されたコントロールワードと前記コピー防止(CP)情報を用いて、マーカ-を発生し、暗号化されたキーを用いてエンクリプションするマーカ-発生及びエンクリプション工程

(4、5)、及び、スクランプリングされたオーディオ及びビデオビットストリームと、エンクリプションされたマーカ-をマルチプレキシングして伝送するマルチプレキシング及び伝送工程(7)によって行われる。

【0050】また、オーディオ及びビデオ信号受信及び記録工程は、伝送されたビットストリームからマーカ-を検出して、暗号化されたキーを用いてディクリプション及び分析して、複写を許容するか否かを決定して、検出されたマーカ-が更新されビデオテープに記録される。マーカ-からコントロールワードが発生してディスクランプリングして、ディスプレイできるように、モニターに出力される。プログラム製作者から伝送されたオーディオ及びビデオ信号は、マーカ-によって記録されたり、ディスプレイされる。

【0051】すなわち、オーディオ及びビデオ信号受信及び記録工程は、図2に示したように、伝送されたビットストリームをディマルチプレキシングして、マーカ-を検出し暗号化されたキーを用いてディクリプションするマーカ-検出工程(11、12)、検出されたマーカ-を分析して複写を許容するか否かを決定しコントロールワードを検出するマーカ-分析工程(13)、検出されたコントロールワードに伝送されたオーディオ及びビデオビットストリームを、ディスクランプリング及びディコーディングして、音声及び映像信号を出力するオーディオ及びビデオディコーディング工程(14、15)、及びマーカ-分析結果複写可能な場合、検出されたマーカ-を更新させ、暗号化されたキーを用いてエンクリプションして挿入するマーカ-挿入工程(16、17、18)によって行われる。

【0052】この過程を詳しく説明すれば次の通りである。まず、プログラム製作者は、オーディオ及びビデオビットストリームをエンコーディングし(1)、スクランプリングのためのコントロールワードを発生した後(2)、発生されたコントロールワードを用いてエンコーディングされたオーディオ及びビデオビットストリームをスクランプリングする(6)。

【0053】次に、不法複写防止のためのコピー防止(CP)情報を発生し(3)、発生されたコントロールワードとコピー防止(CP)情報を用いてマーカ-を発生し(4)、暗号化されたキーを用いてエンクリプションする(5)。

【0054】最後に、スクランプリングされたオーディ

オ及びビデオビットストリームとインクリプションされたマーカ-を、マルチプレキシングして(7)プログラム記録または再生のために伝送する。

【0055】伝送されたビットストリームをディマルチプレキシングしてマーカ-を検出し、(11)、暗号化されたキーを用いて、ディクリプションして、ディクリプションされたマーカ-を出力する(12)。検出されディクリプションされたマーカ-を分析して複写を許容するか否かを決定しコントロールワードを検出する(13)。

【0056】検出されたコントロールワードに伝送されたオーディオ及びビデオビットストリームを、ディスクランプリング及びディコーディングして、音声及び映像信号をモニターに出力してディスプレイできるようにする(14、15)。

【0057】また、マーカ-分析結果複写可能な場合、検出されたマーカ-を更新させ、暗号化されたキーを用いてエンクリプションして、オーディオ及びビデオビットストリームに挿入して記録する(16、17、18)。

【0058】ここで、図3に基づいて、マーカ-が挿入される位置を見る。伝送されるビットストリームは、固定長、すなわち188バイトからなる伝送パケットより構成される。そのうち、ビットストリームの前端に伝送ヘッダが位置する。伝送ヘッダは、再び4バイトの固定長フィールドと可変長のアダプテーションフィールド(adaptation field)に分かれる。そして、アダプテーションフィールド内の1フィールドであって、伝送プライベートデータフィールドが存在する。伝送プライベートデータフィールドは、再びIDフィールドとエンクリプションされた状態のマーカ-より構成される。IDフィールドは、伝送プライベートデータフィールドが本発明の複写防止方法のために用いられるフィールドであることを知らせるための識別子の機能を有し、IDフィールド以後に存在するエンクリプションされたマーカ-により本発明の複写防止機能を実現する。

【0059】マーカ-が暗号化されたキーを用いてディクリプションされれば、マーカ-は、不法複写防止のためのコピー防止(CP)情報が記録されたコピー防止(CP)情報領域と、ディスクランプリングのためのコントロールワードCWが記録されたコントロールワード領域と、リザーブド(Reserved)領域に分かれる。すなわち、ディクリプションされたマーカ-は8バイトよりなり、1バイトよりなるコピー防止(CP)情報領域と3バイトよりなるリザーブド領域と4バイトよりなるコントロールワード領域に分かれる。

【0060】ここで、コピー防止(CP)情報はプログラムの複写可能回数を制限する世代複写制御フィールドを含めてフォーマッティングされるが、世代複写制御フィールドはプログラムの複写を許容する回数を制限する

10

20

30

40

50



ための許容世代フィールドと、複写されたプログラムの現在の世代を示す現在世代フィールドよりなる。

【0061】次に、オーディオ及びビデオ信号受信及び記録工程のマーカ分析工程(13)を詳しく説明する。マーカ分析工程(13)は検出されたマーカから不法複写防止のためのCP情報を検出するコピー防止(CP)情報検出工程、検出されたコピー防止(CP)情報内のプログラムの複写を許容する回数を制限するための許容世代フィールドの許容世代と、複写されたプログラムの現在の世代を示す現在世代フィールドの現在世代とを比較して、複写できるか否かを判別して処理する複写回数制限工程、及び検出されたマーカからディスクランプリングのためのコントロールワードを検出するコントロールワード検出工程により行われる。すなわち、検出されたマーカから不法複写防止のためのコピー防止(CP)情報を検出し、検出されたコピー防止(CP)情報内のプログラムの複写を許容する回数を制限するための許容世代フィールドの許容世代と、複写されたプログラムの現在の世代を示す現在世代フィールドの現在世代とを比較して、複写可能か否かを判別する。複写の可能な場合、記録させ、複写が不可能な場合は、記録しても再生を不可能にさせる。

【0062】次いで、検出されたマーカからディスクランプリングのためのコントロールワードを検出する。ここで、複写回数制限工程は許容世代フィールドの許容世代と、現在世代フィールドの現在世代とを比較して、許容世代が現在世代以下かを判断する工程と、及び判断結果として、許容世代が現在世代以下なら複写が不可能にする工程と、及び判断結果として、許容世代が現在世代以下でなければ複写可能にし、マーカ挿入工程に進む工程により行われる。

【0063】上記の複写回数制限工程を説明すれば次の通りである。

【0064】プログラム製作者が設定した許容世代フィールドの許容世代と、現在の複写回数を示す現在世代フィールドの現在世代とを比較して、許容世代が現在世代以下なら、プログラム製作者が設定した複写回数を超えたので複写をこれ以上不可能にする。この際、複写を不可能にする方法は、複写後再生を不可能にコントロールワードを破壊したり、出力できないようにすることである。なぜなら、オーディオ及びビデオビットストリームは、スクランプリングされた状態で記録されるので、コントロールワードがなければ、スクランプリングされたオーディオ及びビデオビットストリームをディスクランプリングできないからである。

【0065】従って、コントロールワードを破壊すれば、オーディオ及びビデオビットストリームが記録されても再生してディスプレイできないので、記録が不可能なことが同様になる。この際、コントロールワードは周期的に、すなわち0.6秒間隔に変わるので、次に現れ

るコントロールワードを全部破壊することにより複写されても再生を不可能にする。また、ビデオテープ内のコントロールトラックを破壊して複写を不可能にすることもできる。

【0066】一方、マーカは、コントロールワードが変わる毎にビットストリーム内のプライベートデータフィールドに位置することになる。ここで、コントロールワードは周期的に変わるのでコントロールワードが変わって入力される毎にコントロールワードが含まれたマーカが入力される。

【0067】一方、マーカ挿入工程は、マーカ分析結果複写可能な場合はマーカを更新させる工程(16)、更新されたマーカを暗号化されたキーを用いてエンクリプションする工程(17)、及びエンクリプションされたマーカを次に現れるマーカと交替して挿入する工程(18)により行われる。すなわち、マーカ分析結果複写可能な場合は現在世代フィールドの現在世代を"1"増加させ更新させることによりマーカを更新させる(16)。すなわち、現在世代が"1"増加され更新された現在世代フィールドを含むCP情報はコントロールワードと合わせて更新されたマーカとなる。

【0068】更新されたマーカは、再び暗号化されたキーを用いてエンクリプションされ(17)、次に現れるマーカと交替され挿入される。すなわち、マーカは、コントロールワードが変わる毎に入力されるので、コントロールワードが変わる毎に挿入される。言い換えれば、図3に示したようにエンクリプションされたマーカを検出することと、更新されたマーカを交替するのは、時間的に共になされるべきである。

【0069】一方、マーカをエンクリプション及びディクリプションさせるための暗号化されたキーは、一定間隔に別途の伝送路を通じて伝送され貯蔵された後使われることにより不法複写を完璧に防止しうる。すなわち、マーカは、暗号化されたキーでエンクリプションされた状態でビットストリームと共に伝送され記録される。スクランプリングされたオーディオ及びビデオビットストリームをディスクランプリングするためのコントロールワードが、マーカに含まれているので、コントロールワードを得るためには、まずマーカをディクリプションすべきである。ところが、マーカをディクリプションするための暗号化キーが周期的に変化されるので、暗号化キーなしでマーカをディクリプションするのは不可能である。このことによって、不法的にコントロールワードを得ることはさらに難しい。

【0070】本発明によるデジタル磁気記録再生システムの複写防止装置は、図4に示すように、マーカ検出及び挿入部21、ディスクランブラ24、マーカ分析及び処理部22、及びバッファ23より構成される。

【0071】マーカ検出及び挿入部21は、入力され

るビットストリームからマーカを検出し、バッファ23から出力される更新されたマーカを、すなわち更新されエンクリプションされたマーカを、入力されるビットストリームに挿入して出力する。

【0072】マーカ分析及び処理部22は、暗号化されたキーを用いてマーカ検出及び挿入部21から出力されるエンクリプションされたマーカを、ディクリプションし、分析する。このことによって、ビットストリームをディスクランプリングさせるためのコントロールワードを出力する。それから、ディクリプションされたマーカは、更新され、再び暗号化されたキーを用いてエンクリプションされ出力される。

【0073】バッファ23は、マーカ分析及び処理部22から出力されるコントロールワードCWと、更新されエンクリプションされたマーカIEMとをバッファリングする。更新されエンクリプションされたマーカIEMは、マーカ検出及び挿入部21で挿入できるように出力される。

【0074】ディスクランブラ24は、バッファ23から出力されるコントロールワードを用いて、マーカ検出及び挿入部21を通じて出力されるビットストリームを、ディスクランプリングしてディスプレイできるようにモニターに出力したり、マーカが挿入されたビットストリームを記録できるようにDVCRに出力する。ここで、暗号化されたキーは、本発明によるデジタル記録再生システムの複写防止方法のように、一定間隔に別途の伝送路を通じて伝送され貯蔵され著作権の保護効果を倍加させる。

【0075】このように構成されたデジタル磁気記録再生システムの複写防止装置の動作を説明する前に、図3に基づき伝送ビットストリーム及びマーカの構造について説明する。

【0076】デジタル磁気記録再生システムの複写防止装置において、デジタル磁気記録再生システムの複写防止方法と同様に、図3に示したように、マーカは、ビットストリーム内の伝送プライベートデータフィールド(Transfer-private-data-field)に位置している。なお、デジタル磁気記録再生システムの複写防止装置は、不法複写防止のためのCP情報の記録されたCP情報領域と、ディスクランプリングのためのコントロールワードCWが記録されたコントロールワード領域とを含んでいる。

【0077】ここで、CP情報は、プログラムの複写可能回数を制限する世代複写制御フィールドを含むフォーマッティングされる。世代複写制御フィールドは、プログラムの複写を許容する回数を制限するための許容世代フィールドと、複写されたプログラムの現在の世代を示す現在世代フィールドよりなる。また、マーカは8バイトよりなり、このうちCP情報領域は1バイトよりなり、コントロールワード領域は4バイトよりなる。

【0078】次いで、本発明によるデジタル磁気記録再生システムの複写防止装置の概略的な動作を図4に基づいて説明する。

【0079】まず、入力されるビットストリームをモニターにディスプレイする過程を説明する。入力されるビットストリームは、マーカ検出及び挿入部21でマーカが検出されエンクリプションされた状態で、マーカ分析及び処理部22に入力される。エンクリプションされたマーカEMは、マーカ分析及び処理部22で暗号化されたキーを用いてディクリプションされてから分析される。この際、分析されたマーカからコントロールワードが検出されビットストリームをディスクランプリングさせるために、バッファ23をバッファリングされた後ディスクランブラ24に入力される。

【0080】マーカ検出及び挿入部21から、マーカが検出された後のビットストリームは、ディスクランブラ24でバッファ23から出力されるコントロールワードによりディスクランプリングされた後、ディスプレイできるようにモニターに出力される。

【0081】次いで、入力されるビットストリームをDVCRを通じて記録する過程を説明する。入力されるビットストリームからマーカを検出し分析する過程は、同一である。すなわち、入力されるビットストリームは、マーカ検出及び挿入部21でマーカが検出されエンクリプションされた状態で、マーカ分析及び処理部22に入力される。

【0082】コントロールワードを検出するため、エンクリプションされたマーカEMは、マーカ分析及び処理部22で暗号化されたキーを用いてディクリプションされた後分析される。この際、分析結果によって、記録できるようになったり、不可能になる。記録が不可能な場合は、検出されたコントロールワードを破壊して、記録されても再生が不可能になる。記録が可能な場合は、マーカ内の現在世代フィールドの現在世代を"1"増加させ更新させた後、暗号化されたキーを用いてエンクリプションさせバッファ23に出力する。更新されエンクリプションされたマーカは、バッファ23でバッファリングされた後、マーカ検出及び挿入部21に出力され入力されるビットストリームに挿入される。

【0083】一方、コントロールワードは、周期的に、すなわち0.6秒間隔に変化する。マーカは、コントロールワードが変わる毎にビットストリーム内の伝送プライベートデータフィールドに位置することになる。よって、更新されエンクリプションされたマーカは、次に現れるマーカと交替して挿入される。更新されエンクリプションされたマーカが挿入されたビットストリームは、ディスクランブラ24をそのまま通過してDVCRで記録できるように出力される。

【0084】このように構成されるデジタル磁気記録

再生システムの複写防止装置の細部構成及び動作を添付した図面に基いて説明する。図5は、図4の細部構成を示した細部構成図である。各部の細部構成を図5に基いて説明する。

【0085】 マーカー検出及び挿入部21は、入力されるビットストリームからエンクリプションされたマーカーを検出して、マーカー分析及び処理部22に出力する。ビットストリーム内におけるエンクリプションされたマーカーの位置を知らせるマーカー検出フラグ信号は、ディスクランブラ24に出力されて、ディスクランブラ24が初期化される基準信号として使うようにする。ビットストリームを出力するマーカー検出部31、及びマーカー検出部31から出力されるマーカー検出フラグ信号に応じて、マーカー検出部31から出力されるビットストリームに、バッファ23から出力される更新されエンクリプションされたマーカーを挿入してディスクランブラ24に出力するマーカー挿入部32より構成される。

【0086】 マーカー分析及び処理部22は、マーカー検出及び挿入部21のマーカー検出部31から出力されるエンクリプションされたマーカーを暗号化されたキーを用いてディクリプションするマーカー解読部33と、マーカー解読部33から出力されるマーカー内部のCP情報を分析して、複写が許容される場合、バッファ23にコントロールワードを出力しマーカーを更新するための制御信号を出力するマーカー分析部34と、及びマーカー分析部34から出力される制御信号に応じて、マーカー解読部34から出力されるマーカーを更新させ暗号化されたキーを用いてエンクリプションしてバッファ23に出力するマーカー更新及び暗号化部35と、より構成される。ここで、マーカー分析及び処理部22は、暗号化されたキーを貯蔵して、マーカー解読部33とマーカー更新及び暗号化部35に出力する暗号化キー貯蔵部をさらに含めて構成される。

【0087】 また、マーカー分析部34は、CP情報内のプログラムの複写を許容する回数を制限するための許容世代フィールドの許容世代と、複写されたプログラムの現在の世代を示す現在世代フィールドの現在世代とを比較して、複写の可能か否かを判別する。

【0088】 バッファ23は、マーカー分析及び処理部22から出力される更新されエンクリプションされたマーカーを一時貯蔵した後、マーカー検出及び挿入部21に出力するマーカーバッファ36、及びマーカー分析及び処理部22から出力されるコントロールワードを一時貯蔵してから、ディスクランブラ24に出力するコントロールワードバッファ37より構成される。

【0089】 このように構成される本発明によるデジタル磁気記録システムの複写防止装置の動作を図6に基いて説明する。図6(a)は、伝送されたビットストリームのタイミング図である。図6(b)は、マーカー検出フラグ(m-d-e-t-f-l-a-g)のタイミング図であ

る。図6(c)は、マーカー分析部34から出力されるコントロールワードCW(i)のタイミング図である。図6(d)は、マーカー更新及び暗号化部35から出力される更新されエンクリプションされたマーカーIEM(i)のタイミング図である。図6(e)は、マーカーバッファ36から出力される更新されエンクリプションされたマーカーIEM(i)のタイミング図である。図6(f)は、コントロールワードバッファ37から出力されるコントロールワードCW(i)のタイミング図である。伝送されたビットストリーム中には、エンクリプションされたマーカーEM(i)が含まれる。

【0090】 エンクリプションされたマーカーEM(i)を含む伝送されたビットストリームは、図6(a)に示したようになされ、マーカー検出部31に入力され、エンクリプションされたマーカーEM(i)が検出されマーカー解読部33に出力される。また、マーカー検出部31では、エンクリプションされたマーカーの位置を知らせるマーカー検出フラグ信号(m-d-e-t-f-l-a-g)を、図6(b)に示したようにエンクリプションされたマーカーEM(i)部分に発生させ、エンクリプションされたマーカーEM(i)の含まれたビットストリームと共に、マーカー挿入部32に出力し、マーカー検出フラグ(m-d-e-t-f-l-a-g)をディスクランブラ24に出力して、コントロールワードバッファ37から伝送されるコントロールワードCW(i-1)にディスクランブラ24を初期化させる基準信号として使うようにする。エンクリプションされたマーカーEM(i)は、マーカー解読部33で暗号化キーによりディクリプションされ、ディクリプションされたマーカーM(i)に出力される。ディクリプションされたマーカーM(i)はマーカー分析部34で分析され複写可能か否かを判別する。すなわち、マーカー分析部34ではディクリプションされたマーカーM(i)内のCP情報、すなわち、許容世代フィールドと現在世代フィールドとを比較して、許容世代フィールドが現在世代フィールド以下でなければ、複写可能であると判断する。

【0091】 このように複写が許容される場合、マーカー分析部34では、図6(c)に示したように、マーカーM(i)の一部データであるコントロールワードCW(i)をやや遅延させ、コントロールワードバッファ37に出力する。この際、マーカー分析部34では、マーカー更新及び暗号化部35に制御信号を出力して、マーカーを更新させることを制御させる。すなわち、マーカー解読部33では、エンクリプションされたマーカーEM(i)から解読に必要な時間遅延以後、ディクリプションされたマーカーM(i)を作り、マーカー分析部34でディクリプションされたマーカーM(i)から、コントロールワードCW(i)を発生させる。

【0092】 この際、コントロールワードCW(i)は、コントロールワードバッファ37に伝送され、ディ

スクランブラ24で使われるまで貯蔵される。マーカー解読部33から出力されるディクリプションされたマーカーM(i)は、マーカー更新及び暗号化部35でマーカー分析部34から出力される制御信号に応じて更新される。すなわち、更新されるデータは、マーカー内の現在世代フィールドに記録されるデータに、以前に記録された現在世代に"1"を加算してなされる。

【0093】このように更新されたマーカーは、再び暗号化キーによりエンクリプション、すなわち暗号化され図6(c)に示したように、マーカー分析部34から出力されるコントロールワードCW(i)についてやや遅延された状態で、図6(d)に示したようにマーカーバッファ36に出力される。すなわち、マーカー解読部33から出力されるエンクリプションされたマーカーM(i)は、マーカー更新及び暗号化部35に送られ、暗号化に必要な時間遅延以後に更新されエンクリプションされたマーカーIEM(i)に発生されたマーカーバッファ36に伝送される。

【0094】この際、マーカー更新及び暗号化部35と、マーカー分析部34から出力される更新されエンクリプションされたマーカーIEM(i)と、コントロールワードCW(i)が発生する時点と、マーカー挿入部32とディスクランブラ24で更新されエンクリプションされたマーカーIEM(i)とコントロールワードCW(i)を用いる時点、すなわち交替挿入及びディスクランブラ24の初期化過程での時点が不一致するので、この間マーカーバッファ36とコントロールワードマーカーバッファ37でマーカー更新及び暗号化部35とマーカー分析部34から出力される更新されエンクリプションされたマーカーIEM(i)とコントロールワードCW(i)を一時貯蔵する。

【0095】図6(e)に示したように、マーカーバッファ36で一時貯蔵され同期を合わせて出力される更新されエンクリプションされたマーカーIEM(i)は、マーカー挿入部32でマーカー検出部31から出力されるビットストリームに挿入される。すなわち、マーカー挿入部32では、エンクリプションされたマーカーEM(i)が含まれたビットストリームとマーカー検出フラグ信号(m-d e t-e r f l a g)をマーカー検出部31から受信し、エンクリプションされたマーカーEM(i)の位置に交替挿入する更新されエンクリプションされたマーカーIEM(i)をマーカーバッファ36から受信し、図6(e)に示したように、エンクリプションされたマーカーEM(i)を含む伝送されたビットストリーム中のマーカー検出フラグ信号(m-d e t-e r f l a g)の位置に更新されエンクリプションされたマーカーIEM(i)を交替挿入する。

【0096】言い換えれば、マーカー挿入部32は、マーカー検出フラグ信号(m-d e t-e r f l a g)が発生した位置でエンクリプションされたマーカーEM(i)

+1)をマーカーバッファ37から出力される更新されエンクリプションされたマーカーIEM(i)に交替挿入される。

【0097】ここで、交替挿入する更新されエンクリプションされたマーカーIEM(i)は、直前に検出されたエンクリプションされたマーカーから作られたものである。従って、図6(e)に示したように、マーカーバッファ37で一定期間の間貯蔵されてからマーカー挿入部32に出力される。

10 【0098】図6(f)に示したように、コントロールワードバッファ37で一時貯蔵され同期を合わせて出力されるコントロールワードCW(i-1)は、ディスクランブラ24でマーカー挿入部32から出力される伝送されたビットストリームをディスクランプリングするに用いられる。

【0099】この際、ディスクランブラ24は、マーカー検出部31から出力されるマーカー検出フラグ信号(m-d e t-e r f l a g)をコントロールワードバッファ37から出力されるコントロールワードCW(i-1)に初期化させる基準信号とする。すなわち、ディスクランブラ24では、エンクリプションされたマーカーEM(i)が発生された位置、すなわちマーカー検出フラグ信号(m-d e t-e r f l a g)が検出された位置から伝送パケットのペイロード(payload)が始まる前の期間の間、コントロールワードバッファ37から出力されるコントロールワードCW(i-N)に初期化されるべきである。ここで、Nは任意の"0"より大きい自然数であって、コントロールワードCW(i-N)は、エンクリプションされたマーカーEM(i)よりN個以前に伝送されたエンクリプションされたマーカーEM(i-N)から作られたコントロールワードである。この"N"はディスクランブラ24の初期化時点を任意に制御できるようにする。

【0100】

【発明の効果】以上述べたように、本発明は、プログラム供給者が複写防止機能を選択でき、GAフォーマット内に限られたフィールドを用いるので、複写防止機能のための別途のフォーマット変換装置が不要であり、記録するデータ量の増加もないので既存のデジタルVCRを変換させず複写防止機能を行える。

【図面の簡単な説明】

【図1】本発明による複写防止方法のオーディオ及びビデオ信号伝送工程を示す流れ図である。

【図2】本発明による複写防止方法のオーディオ及びビデオ信号受信及び記録工程を示す流れ図である。

【図3】本発明による伝送ストリームの構造図である。

【図4】本発明による複写防止装置の概略的な構成を示すブロック図である。

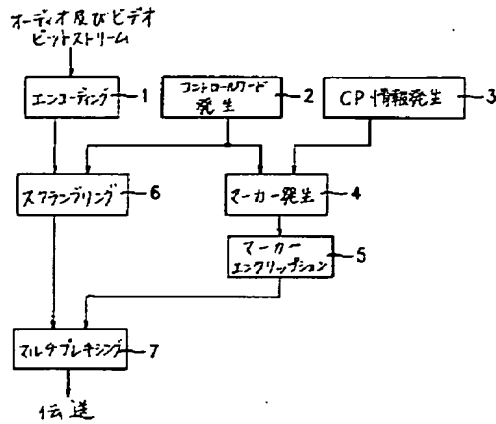
【図5】図4の細部構成を示すブロック図である。

50 【図6】(a)～(f)は、図5の各部の信号波形図である。

## 【符号の説明】

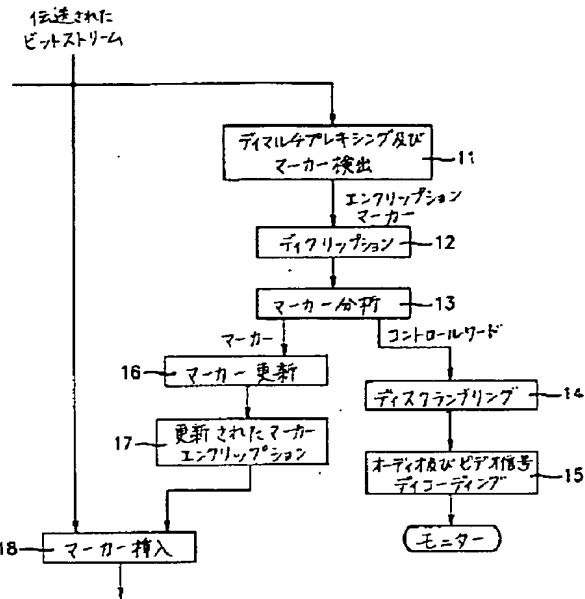
- 21 マーカ－検出及び挿入部  
22 マーカ－分析及び処理部  
23 バッファ部  
24 ディスクランブラ  
31 マーカ－検出部

【図1】

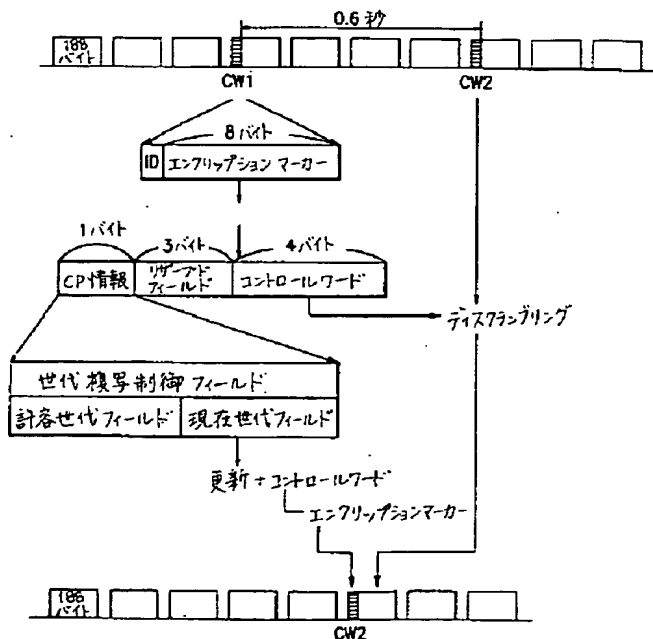


- 32 マーカ－挿入部  
33 マーカ－解読部  
34 マーカ－分析部  
35 マーカ－更新及び暗号化部  
36 マーカ－バッファ  
37 コントロールワードバッファ

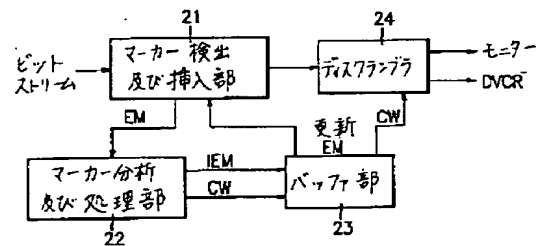
【図2】



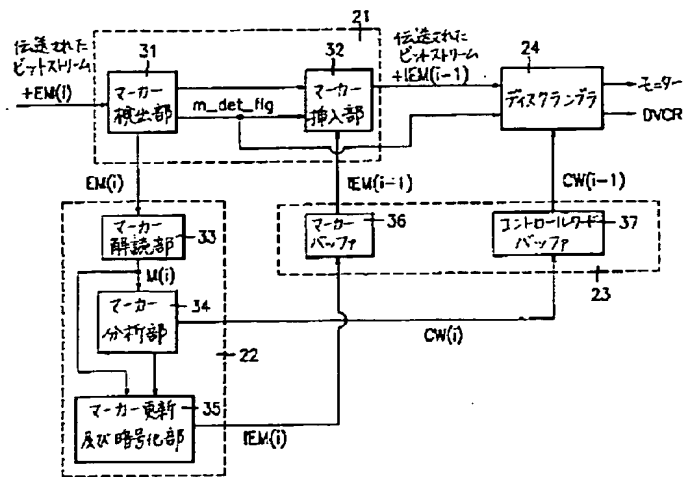
【図3】



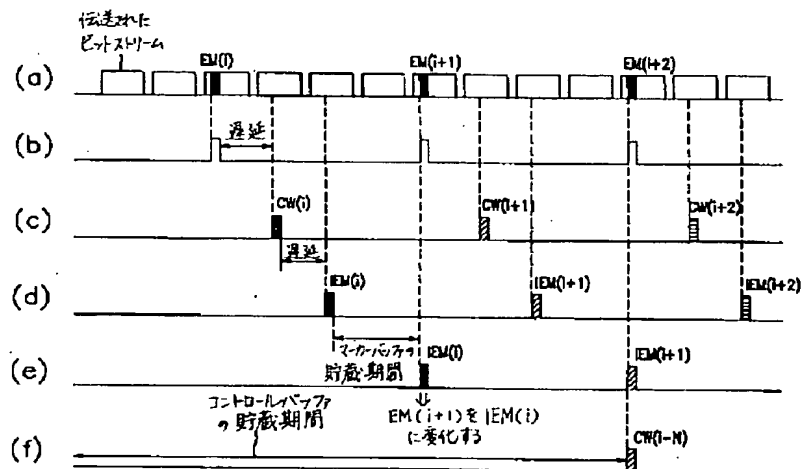
【図4】



【図 5】



【図 6】



DIALOG(R)File 352:DERWENT WPI  
(c)1999 Derwent Info Ltd. All rts. reserv.

010773360 \*\*Image available\*\*

WPI Acc No: 96-270313/199628

Copy prevention method for digital magnetic recording apparatus, esp.  
HDTV VCR - encrypting marker formed by control word for scrambling audio  
and video bit straps, using encoding key to prevent illegal copying,  
multiplexing marker with straps, and detecting marker after transmission

Patent Assignee: LG ELECTRONICS INC (GLDS ); KINSEISHA KK (GLDS )

Inventor: PARK T J

Number of Countries: 006 Number of Patents: 005

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Main IPC	Week
EP 716544	A2	19960612	EP 95308674	A	19951201	H04N-005/913	199628 B
JP 8237596	A	19960913	JP 95318398	A	19951206	H04N-005/91	199647
EP 716544	A3	19970618	EP 95308674	A	19951201	H04N-005/913	199737
US 5689559	A	19971118	US 95566000	A	19951201	H04N-007/16	199801
CN 1131796	A	19960925	CN 95121501	A	19951208	G11B-020/10	199801

Priority Applications (No Type Date): KR 9433336 A 19941208

Cited Patents: No-SR.Pub; EP 267039; EP 498617; EP 580367; EP 581227; EP 589459

Patent Details:

Patent	Kind	Lan	Pg	Filing Notes	Application	Patent
--------	------	-----	----	--------------	-------------	--------

EP 716544	A2	E	16			
-----------	----	---	----	--	--	--

Designated States (Regional): DE FR GB

JP 8237596	A	14
------------	---	----

US 5689559	A	14
------------	---	----

Abstract (Basic): EP 716544 A

The copy prevention method includes an audio and video signal transmitting process which involves encrypting a marker formed (4) by a control word (2) for scrambling (6) audio and video bit straps. An encoding key prevents illegal copying. The marker is multiplexed with the audio and video bit strips scrambled by the control word.

An audio and video signal receiving and recording process detects the marker from the transmitting bit strips, decrypts and analyses it using an encoded key to determined whether copying is permitted or not. The marker is updated and recorded on the video tape. The control word is generated from the marker to perform descrambling and supply the audio and video signals to a monitor for display.

ADVANTAGE - Allows program supplier to select one of several copy prevention functions as required.

Dwg.1/6

Abstract (Equivalent): US 5689559 A

The copy prevention method includes an audio and video signal transmitting process which involves encrypting a marker formed (4) by a control word (2) for scrambling (6) audio and video bit straps. An encoding key prevents illegal copying. The marker is multiplexed with the audio and video bit strips scrambled by the control word.

An audio and video signal receiving and recording process detects the marker from the transmitting bit strips, decrypts and analyses it using an encoded key to determined whether copying is permitted or not. The marker is updated and recorded on the video tape. The control word

is generated from the marker to perform descrambling and supply the audio and video signals to a monitor for display.

ADVANTAGE - Allows program supplier to select one of several copy prevention functions as required.

Dwg.1/6

Derwent Class: W04

International Patent Class (Main): G11B-020/10; H04N-005/91; H04N-005/913;  
H04N-007/16

International Patent Class (Additional): H04N-005/92; H04N-007/167